

SVEUČILIŠTE JOSIPA JURJA STROSSMAYERA U OSIJEKU
ELEKTROTEHNIČKI FAKULTET

Sveučilišni studij

KRIPTOGRAFIJA U RAČUNALSKIM SUSTAVIMA

Završni rad

Marina Perić

Osijek, 2015.

SADRŽAJ:

1. UVOD	1
1.1. Zadatak završnog rada.....	1
2. KLASIČNA KRIPTOGRAFIJA	2
2.1. Osnovni pojmovi	2
2.2. Povijest kriptografije	3
2.3. Supstitucijske šifre	5
2.4. Vigenèreova šifra	8
2.5. Transpozicijske šifre	9
3. RAČUNALNA KRIPTOGRAFIJA.....	11
3.1. Simetrični sustavi za kriptografiju	11
3.1.1. DES algoritam	11
3.1.2. AES alogoritam	13
3.1.3. IDEA algoritam	15
3.2. Asimetrični sustavi za kriptografiju	15
3.2.1. Kriptosustavi s javnim ključem	16
3.2.2. RSA kriptosustav	17
3.2.3. Ostali sustavi s javnim ključem.....	19
3.3. Funkcije za izračunavanje sažetka poruke	19
3.3.1. MD5	19
3.3.2. SHA	21
3.4. Digitalni potpis.....	21
3.5. Kvantna kriptografija	23
4. PRIMJENA KRIPTOGRAFIJE U ELEKTRONSKOJ POŠTI	24
4.1. PGP	25
4.2. S/MIME	27
5. ZAKLJUČAK.....	30
6. LITERATURA	31
7. SAŽETAK.....	32
8. ŽIVOTOPIS.....	33

7. SAŽETAK

Glavni problem kojim sam se bavila u ovome radu bila je primjena kriptografije u računalnim sustavima i u sustavu elektronske pošte. U radu je dan i pregled povijesti kriptografije, a opisani su i principi klasične kriptografije. Računalna kriptografija podjeljena je i opisana kroz simetričnu i asimetričnu, a opisane su i hash funkcije i digitalni potpis. Na kraju, postavljen je problem primjene kriptografije u elektronskoj pošti te je njegovo rješenje dano kroz objašnjenja programa koji se koriste.

CRYPTOGRAPHY IN COMPUTER SYSTEMS

The main problem in this thesis has been the cryptography application in computer and email systems. Besides the usage of cryptography throughout the history, its classical principles have also been described. Two types of cryptography have been portrayed, symmetrical and asymmetrical, as well as the hash functions and digital signature. Finally, the usage of cryptography in the emails has been explained through the applications of different softwares.